ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 330 (2005) 171–191

Theoretical Computer Science

www.elsevier.com/locate/tcs

Explicit test sets for iterated morphisms in free monoids and metabelian groups

Keijo Ruohonen

Institute of Mathematics, Tampere University of Technology, 33101 Tampere, Finland

Abstract

For checking equivalence of any two word morphisms, restricted on a subset (language), it suffices to do this for a finite subset of the language, the so-called finite test set. A way of effectively obtaining a finite test set for a special class of languages, the so-called iterated morphisms, is presented here together with an explicit upper bound for its size. The method can be extended to free metabelian groups, and to certain other metabelian groups.

MSC: 68Q45; 20M35; 20F10

Keywords: Test set; Iterated morphism; HD0L equivalence

1. Introduction

Test sets were originally considered for free finitely generated monoids. We say that a subset S of a language $L \subseteq \Sigma^*$ is a *test set* for L if, for any morphisms $f, g : \Sigma^* \longrightarrow \Delta^*$, the equation

$$f(w) = g(w)$$

holds for all words w in L if and only if it holds for all words in S. This concept can be generalized to other semigroups in an obvious way.

E-mail address: keijo.ruohonen@tut.fi (K. Ruohonen).

0304-3975/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2004.09.017

In 1985 Albert and Lawrence [1] and Guba [8] independently proved the famous

Theorem 1 (*Ehrenfeucht's Conjecture*). *In free finitely generated monoids every language has a finite test set.*

Both proofs are quite short and are based on Hilbert's Basissatz, the proof in [1] via the finite basis property of normal subgroups of finitely generated metabelian groups (see [9]). Moreover, both proofs in fact generalize the conjecture to groups, the proof in [8] to free finitely generated groups and the proof in [1] to finitely generated metabelian groups. The problem of effectively finding these finite test sets for an effectively given L or estimating their sizes has attracted a lot of interest, we refer to the chapter on morphisms in [26], [18, Chapter 14], and [22].

A special case of interest is iterated morphisms. Indeed, much of the initial interest in checking morphism equivalence stemmed from investigation of iterated morphisms. In a free finitely generated monoid Σ^* an *iterated morphism* is a language of the form

$$\{\delta^n(w) \mid n \geqslant 0\},$$

where $\delta : \Sigma^* \longrightarrow \Sigma^*$ is an endomorphism and $w \in \Sigma^*$. Again the concept is immediately generalized to other semigroups. In addition to being theoretically interesting, iterated morphisms have found numerous but scattered uses and applications, the best known undoubtedly being their use in modelling plant-like forms in computer graphics (the Lindenmayer system formalism), see e.g. [23] or Chapter 9 of [27]. In Lindenmayer system theory iterated morphisms are called D0L languages, see [25] and the relevant chapters of [26].

It follows immediately from the proof in [1], via an embedding of Σ^* in the free metabelian group generated by Σ and using group-theoretic enumeration, that finite test sets can be found effectively for iterated morphisms in free finitely generated monoids, and in finitely generated metabelian groups as well, since they have a decidable word problem (see [2]). [1] Indeed, with a bit of care and use of Gröbner bases, a somewhat practicable algorithm for finding a finite test set can be devised along these lines, see [29].

It is known that for iterated morphisms in free finitely generated monoids Σ^* a worst-case lower bound for the size of a finite test set is $\Omega(m^4)$ where m is the size of Σ, see [21]. The only known upper bound, again for the case of finitely generated monoids, is obtainable in an unpublished report of ours [28]. This upper bound is truly huge (the proof uses van der Waerden's Theorem) and involves parameters other than m. On the other hand, its derivation does not use Hilbert's Basissatz.

It is the purpose of this paper to take the basic idea in [28], reformulate it via a group representation, and avoid the use of van der Waerden's Theorem. In this way, compared to [28],

- the construct is shorter and much simpler;
- an explicit upper bound for the size of the test set can be stated that is much smaller (but still quite large and involving parameters other than m), indeed it is even much smaller than

[1] For finitely generated free groups finite test sets of iterated morphisms can be found effectively, too, using the fact that the universal theory of these groups is decidable (see [20]).

the well-known upper bound derived in [7] for the D0L sequence equivalence problem, a very special case of the general problem;

- the result is extended to certain metabelian groups, notably free finitely generated metabelian groups.

The finite test sets we obtain are of the special form $\{\delta^n(w) \mid 0 \leqslant n \leqslant N\}$ and an explicit formula for N is given, see Theorem 11.

In Lindenmayer system theory finding finite test sets for iterated morphisms in free finitely generated monoids is intimately connected with solution of a certain equivalence problem, the so-called HD0L sequence equivalence problem. The upper bound we obtain then gives a new complexity bound for this problem and its special case, the D0L sequence equivalence problem.[2] An HD0L sequence is a sequence of the form

$$(f\delta^n(w))_{n=0}^{\infty},$$

where $\delta : \Sigma^* \longrightarrow \Sigma^*$ is an endomorphism, $w \in \Sigma^*$ and $f : \Sigma^* \longrightarrow \Delta^*$ is a morphism. The concept is naturally extended to all semigroups and groups. It then corresponds to the concept of a linear recurrent sequence in Abelian monoids and groups—considered as $\mathbb{Z}$-(semi)modules—and is thus quite natural even outside Lindenmayer system theory—see [29] and Section 3.

For basics in algebra we refer to [24,15], actually very little algebra is needed here.

2. Basics of $\mathbb{Z}$-rational sequences: an overview

The gist of our construct is based on properties of $\mathbb{Z}$-rational sequences. We give here an overview without proofs. $\mathbb{Z}$-rational sequences—as coefficient sequences of $\mathbb{Z}$-rational formal power series—are widely discussed e.g. in [30] and [4].

A *$\mathbb{Z}$-rational sequence* is a sequence $(f_n)_{n=0}^{\infty}$ satisfying a linear homogeneous recurrence with constant coefficients (LHRCC in short)

$$f_n = c_1 f_{n-1} + c_2 f_{n-2} + \cdots + c_k f_{n-k} \quad \text{for } n \geqslant k,$$

where the coefficients $c_1, c_2, \ldots, c_k$ and the initial values $f_0, f_1, \ldots, f_{k-1}$ are integers. k is the *order* of the LHRCC. The *characteristic polynomial* of the LHRCC is the monic polynomial

$$\chi(r) = r^k - c_1 r^{k-1} - \cdots - c_{k-1} r - c_k \in \mathbb{Z}[r].$$

The roots of χ are the *characteristic roots* of the LHRCC. (We exclude the trivial case where $k = 0$.)

[2] In certain significant cases solution of the HD0L language equivalence problem, i.e., equivalence of sets of terms of HD0L sequences, can be reduced to the sequence equivalence problem. Especially, equivalence of D0L languages can be reduced to the D0L sequence equivalence problem. See [14,25]. The general case of the HD0L language equivalence problem is open.

It is well-known that f_n has the *exponential polynomial representation*

$$f_n = \sum_{j=1}^{l_1} p_j(n)\rho_j^n + \sum_{j=l_1+1}^{l_2} p_j(n)(-1)^n\rho_j^n + \sum_{j=l_2+1}^{l_3} \rho_j^n \left(p_j(n)\mathrm{e}^{\mathrm{i}n\phi_j} + \overline{p_j(n)}\mathrm{e}^{-\mathrm{i}n\phi_j} \right) \quad \text{for } n \geqslant n_0,$$

where

- the numbers $\rho_1, \ldots, \rho_{l_3}$ are positive reals,
- $\rho_1, \ldots, \rho_{l_1}$ are the distinct positive real roots of χ (if any), and p_j is a polynomial with real coefficients of degree less than the multiplicity of the root ρ_j $(j = 1, \ldots, l_1)$,
- $-\rho_{l_1+1}, \ldots, -\rho_{l_2}$ are the distinct negative real roots of χ (if any), and p_j is a polynomial with real coefficients of degree less than the multiplicity of the root $-\rho_j$ $(j = l_1 + 1, \ldots, l_2)$,
- $\rho_{l_2+1}\mathrm{e}^{\pm\mathrm{i}\phi_{l_2+1}}, \ldots, \rho_{l_3}\mathrm{e}^{\pm\mathrm{i}\phi_{l_3}}$ are the distinct complex conjugate root pairs of χ (if any), and p_j is a polynomial with complex coefficients of degree less than the multiplicity of the root pair $\rho_j\mathrm{e}^{\pm\mathrm{i}\phi_j}$ $(j = l_2 + 1, \ldots, l_3)$,
- $\phi_{l_2+1}, \ldots, \phi_{l_3} \in (0, \pi)$,
- n_0 is the multiplicity of zero as a root of χ.

This representation is unique. Indeed, the coefficients of the exponential polynomial representation are uniquely determined by a linear system of equations the matrix of which is the Casoratian matrix of the terms of the representation.

We need the representation in the real form

$$f_n = \sum_{j=1}^{l_1} p_j(n)\rho_j^n + \sum_{j=l_1+1}^{l_2} p_j(n)\rho_j^n \cos n\pi + \sum_{j=l_2+1}^{l_3} \rho_j^n (p_{1j}(n)\cos n\phi_j + p_{2j}(n)\sin n\phi_j) \quad \text{for } n \geqslant n_0,$$

where p_{1j} and p_{2j} are polynomials with real coefficients of degree less than the multiplicity of the root pair $\rho_j\mathrm{e}^{\pm\mathrm{i}\phi_j}$ $(j = l_2 + 1, \ldots, l_3)$. Again the representation is unique. This can be extended to $\mathbb{R}$ in the form

$$f(x) = \sum_{j=1}^{l_1} p_j(x)\rho_j^x + \sum_{j=l_1+1}^{l_2} p_j(x)\rho_j^x \cos x\pi + \sum_{j=l_2+1}^{l_3} \rho_j^x (p_{1j}(x)\cos x\phi_j + p_{2j}(x)\sin x\phi_j).$$

Then $f_n = f(n)$ and $f(x)$ satisfies the difference equation

$$f(x) = c_1 f(x-1) + c_2 f(x-2) + \cdots + c_k f(x-k).$$

Especially, if $(f_n)_{n=0}^{\infty}$ is the zero sequence, then the extension $f(x)$ is the zero function. (It may be noted that the difference equation may have other solutions: for instance, the nonzero function $\sin \pi x$ satisfies the difference equation $f(x) = -f(x-1)$. Of course, $\sin n\pi = 0$ and $\sin \pi x$ is not an allowed extension here.)

$\mathbb{Z}$-rational sequences $(f_n)_{n=0}^{\infty}$ can be identified with integer sequences having a *matrix representation*, i.e., a representation of the form

$$f_n = \mathbf{e}^{\mathrm{T}}\mathbf{M}^n\mathbf{d} \quad \text{for } n \geqslant 0,$$

where, for some k, $\mathbf{e}$ and $\mathbf{d}$ are k-vectors with integer entries and $\mathbf{M}$ is a $k \times k$-matrix with integer entries. (Indeed, a matrix representation corresponding to the LHRCC is obtained using the companion matrix of its characteristic polynomial, and an LHRCC corresponding to a matrix representation is obtained from the characteristic polynomial of the matrix $\mathbf{M}$ via the Cayley–Hamilton Theorem.)

A *p-decomposition* of a $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$, satisfying an LHRCC of order k, is the collection of sequences

$$(f_{pn+j})_{n=0}^{\infty} \quad (j = k, \ldots, k+p-1).$$

(Note that the first k terms of $(f_n)_{n=0}^{\infty}$ are excluded in order to get rid of initial values that do not affect later terms.) The sequences $(f_{pn+j})_{n=0}^{\infty}$ are the *components* of the p-decomposition—also called decimations, see [6]—and, as is easily seen using a matrix representation, they are $\mathbb{Z}$-rational sequences satisfying the same LHRCC of order k and not having zero as its characteristic root.

We then turn to properties concerning the zero terms in a $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$. A fundamental result is

Theorem 2 (*Skolem–Mahler–Lech*). *If the $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$ contains zero terms then there exist nonnegative integers $a_1, \ldots, a_L$ and $b_1, \ldots, b_L$ such that*:

$$\{n \mid f_n = 0\} = \{a_j n + b_j \mid n \geqslant 0 \text{ and } j = 1, \ldots, L\}.$$

Moreover, each nonzero a_j divides the lcm C of the orders of those primitive roots of unity which can be expressed as ratios of two roots of the characteristic polynomial χ.

The theorem was first proved using p-adic methods (see e.g. [17]), an elementary proof was obtained by Hansel [10]. The latter part of the theorem is an easy consequence of the first part. Berstel and Mignotte [3] showed that

Lemma 3. $C \leqslant e^{2k\sqrt{3\ln k}}$.

This of course implies that it is decidable whether or not a $\mathbb{Z}$-rational sequence has infinitely many zero terms. On the other hand, it is a famous open problem whether it is decidable if a $\mathbb{Z}$-rational sequence has a zero term. The problem is known to be NP-hard (see [5]), and decidable in the special case $k \leqslant 3$ (see [32]). Remarkably, an upper bound is known for the number of zero terms, if finite, which depends only on k (and is triply exponential in k, see [31]).

We say that a $\mathbb{Z}$-rational sequence has the *finite-zeros property* if it either is identically zero or has only finitely many zero terms.

Lemma 4. *The components of a p-decomposition of $(f_n)_{n=0}^{\infty}$ where C divides p have the finite-zeros property*.

Proof. This follows from the Skolem–Mahler–Lech Theorem. The components cannot have only finitely many nonzero terms as is seen by applying the LHRCC backwards. □

Suppose then that we have a doubly indexed collection of $\mathbb{Z}$-rational sequences

$$\mathcal{S} : \left(f_n^{(jl)}\right)_{n=0}^{\infty} \quad (j = 1, \ldots, L; l = 1, \ldots, M_j),$$

each satisfying the same LHRCC $\mathcal{L}$. We say that the sequence $(F_n)_{n=0}^{\infty}$ defined by

$$F_n = \prod_{j=1}^{L} \sum_{l=1}^{M_j} \left(f_n^{(jl)}\right)^2$$

is the *zero indicator* of $\mathcal{S}$. It is immediate that we have the logical equivalence

$$F_n = 0 \Longleftrightarrow \bigvee_{j=1}^{L} \bigwedge_{l=1}^{M_j} \left(f_n^{(jl)} = 0\right).$$

Lemma 5. *The zero indicator sequence* $(F_n)_{n=0}^{\infty}$ is a $\mathbb{Z}$*-rational sequence satisfying an LHRCC of order*

$$T = \binom{L + D - 1}{D - 1} (2L(s - 1) + 1),$$

where d is the number of distinct characteristic roots of $\mathcal{L}$*, s is the maximum multiplicity of characteristic roots of* $\mathcal{L}$*, and* $D = \frac{1}{2}d(d + 1)$.

Proof. Denote by $\xi_1, \ldots, \xi_d$ the squares of the characteristic roots of $\mathcal{L}$, and by $\xi_{d+1}, \ldots, \xi_D$ the pairwise products of these roots. Using the exponential polynomial representation for the sequences in $\mathcal{S}$ we can then write

$$F_n = \prod_{j=1}^{L} \sum_{i=1}^{D} p_{ij}(n)\xi_i^n$$

for some polynomials p_{ij} of degree at most $2(s - 1)$ with complex coefficients, and further

$$F_n = \sum_{h_1 + \cdots + h_D = L} P_{h_1, \ldots, h_D}(n) \left(\xi_1^{h_1} \cdots \xi_D^{h_D}\right)^n$$

for some polynomials $P_{h_1,\ldots,h_D}$ of degree at most $2L(s - 1)$ with complex coefficients. In the last sum, the number of summands equals the binomial coefficient in the formula for T. We have then an exponential polynomial representation of $(F_n)_{n=0}^{\infty}$ corresponding to an LHRCC of order T with complex coefficients. Since $\mathbb{C}$ is a Fatou extension of $\mathbb{Z}$ (see Theorem 6.2 of [30]), it follows that this LHRCC may be assumed to have integer coefficients. □

Lemma 6. *Assume that all sequences* $\left(f_n^{(jl)}\right)_{n=0}^{\infty}$ *of* $\mathcal{S}$ *have the finite-zeros property. Then so does the sequence* $(F_n)_{n=0}^{\infty}$*. If the sequence* $(F_n)_{n=0}^{\infty}$ *is identically zero then, for some j, the sequences* $\left(f_n^{(jl)}\right)_{n=0}^{\infty}$ $(l = 1, \ldots, M_j)$ *are also identically zero.*

Proof. To prove the first claim assume that all sequences $\left(f_n^{(jl)}\right)_{n=0}^{\infty}$ have the finite-zeros property and that the sequence $(F_n)_{n=0}^{\infty}$ contains infinitely many zero terms. Then, for some j, each of the sequences $\left(f_n^{(jl)}\right)_{n=0}^{\infty}$ $(l = 1, \ldots, M_j)$ also contain infinitely many zero terms. It follows that these sequences are all identically zero, and hence that the sequence $(F_n)_{n=0}^{\infty}$ is also identically zero. The second claim is proved similarly. □

3. Recurrence formulation of iterated morphism

Consider the free metabelian group G_Σ generated by the finite set $\Sigma = \{a_1, \ldots, a_m\}$. An iterated morphism is a subset of G_Σ of the form

$$U = \{\delta^n(w) \mid n \geqslant 0\},$$

where δ is an endomorphism on G_Σ and $w \in G_\Sigma$. We write

$$\delta(a_j) = a_{i_{j1}}^{s_{j1}} \cdots a_{i_{jL_j}}^{s_{jL_j}}, \quad \text{where} \quad s_{j1}, \ldots, s_{jL_j} \in \{-1, 1\}$$

for $j = 1, \ldots, m$, and

$$w = a_{i_1}^{s_1} \cdots a_{i_L}^{s_L}, \quad \text{where} \quad s_1, \ldots, s_L \in \{-1, 1\}.$$

Consider then another free metabelian group G_Δ generated by $\Delta = \{b_1, \ldots, b_r\}$, and two morphisms $f, g : G_\Sigma \longrightarrow G_\Delta$. We get the following recurrence system for the sequence $((f\delta^n(w))(g\delta^n(w))^{-1})_{n=0}^{\infty}$:

$$\begin{aligned}
f\delta^{n+1}(a_j) &= (f\delta^n(a_{i_{j1}}))^{s_{j1}} \cdots (f\delta^n(a_{i_{jL_j}}))^{s_{jL_j}} \ (j = 1, \ldots, m),\\
g\delta^{n+1}(a_j) &= (g\delta^n(a_{i_{j1}}))^{s_{j1}} \cdots (g\delta^n(a_{i_{jL_j}}))^{s_{jL_j}} \ (j = 1, \ldots, m),\\
(f\delta^{n+1}(w))(g\delta^{n+1}(w))^{-1} &= (f\delta^n(a_{i_1}))^{s_1} \cdots (f\delta^n(a_{i_L}))^{s_L}\\
&\quad \times (g\delta^n(a_{i_L}))^{-s_L} \cdots (g\delta^n(a_{i_1}))^{-s_1}.
\end{aligned}$$

To find a finite test set S for U it suffices to find a number N, depending possibly on m, δ and w but not on f or g, such that

$$(f\delta^n(w))(g\delta^n(w))^{-1} = e \quad (n \geqslant 0)$$

whenever

$$(f\delta^n(w))(g\delta^n(w))^{-1} = e \quad (0 \leqslant n \leqslant N),$$

where e is the identity element of G_Δ. We may then take

$$S = \{\delta^n(w) \mid 0 \leqslant n \leqslant N\}.$$

This is the approach we will apply, using the above recurrence system under a polynomial coding. It may be noted that these finite test sets are of a special form, an initial block of the sequence $(\delta^n(w))_{n=0}^{\infty}$, and thus much smaller test sets may well exist. E.g., in the case $m = 2$ it is known that two elements suffice in free monoids, see [11].

Let us then denote by $[v]$ the image of the element $v \in G_\Sigma$ under the canonical morphism mapping G_Σ onto the free abelian group generated by Σ, i.e., the group $\mathbb{Z}^m$, and by $[\delta]$ the endomorphism on $\mathbb{Z}^m$ induced by δ. We use similar notation for the canonical image of G_Δ in $\mathbb{Z}^r$. We may identify $[\delta]$ by an $m \times m$-matrix and $[f]$ and $[g]$ by $r \times m$-matrices with integer entries. Since then

$$[f\delta^n(a_j)] = [f][\delta]^n[a_j], \quad [g\delta^n(a_j)] = [g][\delta]^n[a_j]$$

and

$$[(f\delta^n(w))(g\delta^n(w))^{-1}] = ([f] - [g])[\delta]^n[w]$$

we see that each of the vectorial sequences $([f\delta^n(a_j)])_{n=0}^\infty$ and $([g\delta^n(a_j)])_{n=0}^\infty$ $(j = 1, \ldots, m)$ and $([(f\delta^n(w))(g\delta^n(w))^{-1}])_{n=0}^\infty$ satisfies the same LHRCC of order m, given by the characteristic polynomial of $[\delta]$. It is important that this LHRCC does not depend on f or g. Components of these sequences are thus $\mathbb{Z}$-rational, and we need the properties of $\mathbb{Z}$-rational sequences given in the previous section to deal with them.

4. Polynomial recurrence for iterated morphism

We continue the construct of the previous section. The Magnus representation μ for G_Δ is the polynomial matrix representation given by

$$b_j \rightleftharpoons \mu(b_j) = \begin{pmatrix} 1 & 0 \\ y_j & u_j \end{pmatrix} \quad (j = 1, \ldots, r),$$

where $y_1, \ldots, y_r$ (collectively denoted by $\mathbf{y}$) and $u_1, \ldots, u_r$ (collectively denoted by $\mathbf{u}$) are different polynomial variates, see [19]. Representation of an element v of G_Δ is then of the form

$$v \rightleftharpoons \mu(v) = \begin{pmatrix} 1 & 0 \\ p(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}} \end{pmatrix},$$

where $\mathbf{a}$ is the multi-index $(\alpha_1, \ldots, \alpha_r) = [v]^{\mathrm{T}}$ and

$$p(\mathbf{y}, \mathbf{u}) = \sum_{j=1}^{r} p_j(\mathbf{u}) y_j \quad \text{and} \quad \mathbf{u}^{\mathbf{a}} = u_1^{\alpha_1} \cdots u_r^{\alpha_r}.$$

Here $p_j(\mathbf{u})$ and $\mathbf{u}^{\mathbf{a}}$ are Laurent polynomials with integer coefficients. Group operations are represented by the matrix operations

$$\begin{pmatrix} 1 & 0 \\ p_1(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}_1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p_2(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}_2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p_1(\mathbf{y}, \mathbf{u}) + \mathbf{u}^{\mathbf{a}_1} p_2(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}_1 + \mathbf{a}_2} \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ p(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -\mathbf{u}^{-\mathbf{a}} p(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{-\mathbf{a}} \end{pmatrix}.$$

We now apply the representation to the recurrence system obtained in the previous section. For simplicity we denote

$$\mu(f\delta^n(a_i)) = \begin{pmatrix} 1 & 0 \\ p_{in}(\mathbf{y},\mathbf{u}) & \mathbf{u}^{\mathbf{a}_{in}} \end{pmatrix},$$
$$\mu(g\delta^n(a_i)) = \begin{pmatrix} 1 & 0 \\ p_{m+i,n}(\mathbf{y},\mathbf{u}) & \mathbf{u}^{\mathbf{a}_{m+i,n}} \end{pmatrix} \quad (i = 1,\ldots,m)$$

and

$$\mu((f\delta^n(w))(g\delta^n(w))^{-1}) = \begin{pmatrix} 1 & 0 \\ p_n(\mathbf{y},\mathbf{u}) & \mathbf{u}^{\mathbf{a}_n} \end{pmatrix} \quad (n \geqslant 0).$$

We note that

$$\mathbf{a}_{in}^{\mathrm{T}} = [f\delta^n(a_i)] = [f][\delta]^n[a_i] \quad \text{for } i = 1,\ldots,m,$$
$$\mathbf{a}_{in}^{\mathrm{T}} = [g\delta^n(a_i)] = [g][\delta]^n[a_i] \quad \text{for } i = m+1,\ldots,2m$$

and

$$\mathbf{a}_n^{\mathrm{T}} = [(f\delta^n(w))(g\delta^n(w))^{-1}] = ([f]-[g])[\delta]^n[w],$$

considered as vectorial sequences, all satisfy the same LHRCC of order m given by the characteristic polynomial of the matrix $[\delta]$. We denote this LHRCC by $\mathcal{L}$.

We may then write, taking $\mathbf{u}^{\mathbf{a}_{in}}$ and $\mathbf{u}^{\mathbf{a}_n}$ as known, the recurrence system in the form

$$p_{i,n+1}(\mathbf{y},\mathbf{u}) = \sum_{j=1}^{2m} q_{ijn}(\mathbf{u})\, p_{jn}(\mathbf{y},\mathbf{u}) \quad (i = 1,\ldots,2m),$$
$$p_{n+1}(\mathbf{y},\mathbf{u}) = \sum_{j=1}^{2m} q_{jn}(\mathbf{u})\, p_{jn}(\mathbf{y},\mathbf{u}) \quad (n \geqslant 0).$$

The coefficient polynomials $q_{ijn}(\mathbf{u})$ and $q_{jn}(\mathbf{u})$ are Laurent polynomials with integer coefficients of the form

$$q_{ijn}(\mathbf{u}) = \sum_{l=1}^{M_{ij}} c_{ijl}\mathbf{u}^{\mathbf{a}_{ijln}} \quad \text{and} \quad q_{jn}(\mathbf{u}) = \sum_{l=1}^{M_j} c_{jl}\mathbf{u}^{\mathbf{a}_{jln}},$$

where the (vectorial) sequences $(\mathbf{a}_{ijln})_{n=0}^{\infty}$ and $(\mathbf{a}_{jln})_{n=0}^{\infty}$ all satisfy the LHRCC $\mathcal{L}$.

As was noticed in Section 2, the sequences $(\mathbf{a}_{ijln})_{n=0}^{\infty}$ and $(\mathbf{a}_{jln})_{n=0}^{\infty}$ may then be extended to real (vector)-valued functions denoted by

$$\mathbf{a}_{ijl}(x) \quad \text{and} \quad \mathbf{a}_{jl}(x),$$

respectively, defined on $\mathbb{R}$. This extension can be applied on q_{ijn} and q_{jn}, too, but since we do not want to deal with generalized Laurent polynomials here, we do this only for a fixed positive value $\mathbf{u}_0$ of $\mathbf{u}$. We thus get the functions

$$q_{ij}(\mathbf{u}_0;x) = \sum_{l=1}^{M_{ij}} c_{ijl}\mathbf{u}_0^{\mathbf{a}_{ijl}(x)} \quad \text{and} \quad q_j(\mathbf{u}_0;x) = \sum_{l=1}^{M_j} c_{jl}\mathbf{u}_0^{\mathbf{a}_{jl}(x)}.$$

An important property, useful later on, is that functions of this form are real analytic in $\mathbb{R}$. Thus they either are identically zero or do not have clustered zeros.

The extension may be further applied to the recurrence system above, and a difference system is obtained. Assume first that the initial values are extended to

$$p_i(\mathbf{u}_0, \mathbf{y}; x) \quad (i = 1, \ldots, 2m) \quad \text{and} \quad p(\mathbf{u}_0, \mathbf{y}; x)$$

on some small interval $(0, \varepsilon)$. We may then write the difference system

$$p_i(\mathbf{y}, \mathbf{u}_0; x+1) = \sum_{j=1}^{2m} q_{ij}(\mathbf{u}_0; x)\, p_j(\mathbf{y}, \mathbf{u}_0; x) \quad (i = 1, \ldots, 2m),$$

$$p(\mathbf{y}, \mathbf{u}_0; x+1) = \sum_{j=1}^{2m} q_j(\mathbf{u}_0; x)\, p_j(\mathbf{y}, \mathbf{u}_0; x) \quad \text{for } x \in \bigcup_{n=0}^{\infty} (n, n+\varepsilon).$$

Since dependence on $\mathbf{y}$ is linear, the Euclidean norm can be used and it is immediate that $p_i(\mathbf{y}, \mathbf{u}_0; x)$ and $p(\mathbf{y}, \mathbf{u}_0; x)$ are continuous functions of x, provided that the extended initial values are so. A similar conclusion is valid for the half-open initial interval $[0, \varepsilon)$ and the set $\bigcup_{n=0}^{\infty}[n, n+\varepsilon)$.

5. Properties of coefficient polynomials

We are going to apply an elimination procedure to the polynomial recurrence/difference system described in the previous section. We therefore need basic properties of the coefficient polynomials, it is e.g. imperative to avoid zero values of pivot coefficients used in this elimination.

The coefficients will be Laurent polynomials of the general form

$$q_n(\mathbf{u}) = \sum_{l=1}^{M^+} \mathbf{u}^{\mathbf{a}_{ln}^+} - \sum_{l=1}^{M^-} \mathbf{u}^{\mathbf{a}_{ln}^-},$$

where the sequences $(\mathbf{a}_{ln}^{\pm})_{n=0}^{\infty}$ all satisfy the LHRCC $\mathcal{L}$. We note first that this form of polynomials is closed under addition, subtraction and multiplication. We call $M = \max(M^+, M^-)$ the *max-trace* of q_n. The following properties of max-trace are then immediate:

Lemma 7. (i) max-trace$(q_{1n} \pm q_{2n}) \leqslant$ max-trace(q_{1n}) + max-trace(q_{2n}).
(ii) max-trace$(q_{1n} q_{2n}) \leqslant 2$ max-trace(q_{1n}) max-trace(q_{2n}).

If, for some n, q_n is the zero polynomial then obviously we must have $M^+ = M^- = M$. Furthermore, there exists then an M-permutation s such that

$$\mathbf{a}_{ln}^+ = \mathbf{a}_{s(l)n}^- \quad (l = 1, \ldots, M).$$

To find out whether or not q_n is the zero polynomial, we may go through all $M!$ permutations s and check the above equations, component by component. This leads to a collection of $\mathbb{Z}$-rational sequences

$$\mathcal{S} : \left(f_n^{(jt)}\right)_{n=0}^{\infty} \quad (j = 1, \ldots, M!; t = 1, \ldots, rM),$$

each satisfying the LHRCC $\mathcal{L}$ of order m, and its zero indicator

$$F_n = \prod_{j=1}^{M!} \sum_{t=1}^{rM} \left(f_n^{(jt)} \right)^2,$$

see Section 2. Now, q_n is the zero polynomial if and only if $F_n = 0$. We call $(F_n)_{n=0}^{\infty}$ the *zero indicator of the polynomial sequence* $(q_n)_{n=0}^{\infty}$. To include all cases, we define F_n to be identically equal to 1 if $M^+ \neq M^-$. By Lemma 5, the zero indicator sequence $(F_n)_{n=0}^{\infty}$ satisfies an LHRCC of order

$$T = \binom{M! + D - 1}{D - 1} (2(s-1)M! + 1),$$

where s is the maximum multiplicity of characteristic roots of $\mathcal{L}$, $D = \frac{1}{2}d(d+1)$ and d is the number of distinct characteristic roots of $\mathcal{L}$. Thus, if the sequence $(q_n)_{n=0}^{\infty}$ contains T consecutive zero polynomial terms it has only finitely many nonzero polynomial terms, which must appear before these zero polynomial terms.

We say that the sequence $(q_n)_{n=0}^{\infty}$ has the *finite-zeros property* if it either consists of zero polynomials only, or then has only finitely many zero polynomial terms. We have immediately

Lemma 8. *The sequence $(q_n)_{n=0}^{\infty}$ has the finite-zeros property if and only if its zero indicator sequence $(F_n)_{n=0}^{\infty}$ has this property.*

By Lemmas 4, 6 and 8, the finite-zeros property of all coefficient polynomial sequences $(q_n)_{n=0}^{\infty}$ can be guaranteed by an appropriate choice of the LHRCC $\mathcal{L}$, more specifically, by taking a proper decomposition. Indeed, we will assume that such a decomposition is made, whence *all coefficient polynomial sequences will have the finite-zeros property.*

Assuming, as indicated, that a coefficient polynomial sequence $(q_n)_{n=0}^{\infty}$ has the finite-zeros property, it either is identically equal to the zero polynomial or it has only finitely many zero polynomial terms. Fixing the variable $\mathbf{u}$ to a positive value $\mathbf{u}_0$ and extending the multi-indices to $\mathbb{R}$ we obtain the real analytic function

$$q(\mathbf{u}_0; x) = \sum_{l=1}^{M^+} \mathbf{u}_0^{\mathbf{a}_l^+(x)} - \sum_{l=1}^{M^-} \mathbf{u}_0^{\mathbf{a}_l^-(x)}.$$

We have then the following basic property:

Lemma 9. *If the sequence $(q_n)_{n=0}^{\infty}$ is identically zero then, for any positive $\mathbf{u}_0$, $q(\mathbf{u}_0; x)$ is the zero function.*

Proof. If the sequence $(q_n)_{n=0}^{\infty}$ is identically zero then its zero indicator $(F_n)_{n=0}^{\infty}$ is also identically zero and $M^+ = M^- = M$. By Lemma 6, it follows that for some M-permutation s:

$$\mathbf{a}_{ln}^+ = \mathbf{a}_{s(l)n}^- \quad (l = 1, \ldots, M)$$

holds for all n and thus the differences

$$\mathbf{a}_l^+(x) - \mathbf{a}_{s(l)}^-(x) \quad (l = 1, \ldots, M)$$

are identically zero. □

If the sequence $(q_n)_{n=0}^{\infty}$ is not identically zero, then we may fix the variable $\mathbf{u}$ to a positive value $\mathbf{u}_0$ such that $q_n(\mathbf{u}_0) \neq 0$ for some n and we get the real analytic function $q(\mathbf{u}_0; x)$ which is not identically zero and thus does not have clustered zeros. Therefore we have

Lemma 10. *Assume that $q_n(\mathbf{u}_0) \neq 0$ for some n. Then for any fixed positive integer N, there exists a positive number ε_N such that $q(\mathbf{u}_0; x) \neq 0$ for $x \in \bigcup_{n=0}^{N}(n, n + \varepsilon_N)$.*

We can thus relatively freely work in sets of the form $\bigcup_{n=0}^{N}(n, n+\varepsilon_N)$ and then consider limits at $x \to n+$.

6. Elimination procedure

We assume, as told in the previous section, that a decomposition is made to force the finite-zeros property. By Lemma 3, this can be achieved by replacing δ by $\delta^{K!}$ where

$$K = \left\lfloor e^{2m\sqrt{3 \ln m}} \right\rfloor$$

and considering in turn the initial elements

$$\delta^j(w) \quad (j = m, \ldots, m + K! - 1).$$

We begin with the difference system

$$p_i(\mathbf{y}, \mathbf{u}_0; x + 1) = \sum_{j=1}^{2m} q_{ij}(\mathbf{u}_0; x)\, p_j(\mathbf{y}, \mathbf{u}_0; x) \quad (i = 1, \ldots, 2m),$$

$$p(\mathbf{y}, \mathbf{u}_0; x + 1) = \sum_{j=1}^{2m} q_j(\mathbf{u}_0; x)\, p_j(\mathbf{y}, \mathbf{u}_0; x) \quad \text{for } x \in \bigcup_{n=N_0}^{N} (n, n + \varepsilon_N)$$

described in Section 4. Note the range of n. The choice of $\mathbf{u}_0$, to be indicated later, will be such that by Lemma 10 we may choose an arbitrarily large $N \geqslant N_0 + 2m$ by adjusting ε_N accordingly. The choice of N_0 will be explained later. The aim of the elimination procedure is to get a difference equation for $p(\mathbf{y}; \mathbf{u}_0, x)$ which does not involve the components $p_i(\mathbf{y}; \mathbf{u}_0, x)$ $(i = 1, \ldots, 2m)$. Without reducing generality we may assume that these components appear as pivot elements in the order $p_1, p_2, \ldots, p_t$. Note that not all components need appear as pivot elements. For simplicity of notation we ignore $\mathbf{u}_0$ and $\mathbf{y}$. The procedure is the following:

(1) For p_1 to appear as the first pivot element, $q_{1n}(\mathbf{u})$ must not be identically zero. The first step is to solve the last equation for $q_1(x)\, p_1(x)$, multiply the other equations by

$q_1(x)$ and then substitute the result in them

$$\begin{aligned} q_1(x)p_i(x+1) &= q_{i1}(x)\left(p(x+1) - \sum_{j=2}^{2m} q_j(x)p_j(x)\right) + \sum_{j=2}^{2m} q_{ij}(x)q_1(x)p_j(x) \\ &= q_{i1}(x)p(x+1) + \sum_{j=2}^{2m} (q_{ij}(x)q_1(x) - q_{i1}(x)q_j(x))p_j(x) \\ &= q_{i1}(x)p(x+1) + \sum_{j=2}^{2m} q_{ij}^{(1)}(x)p_j(x) \quad (i = 1, \ldots, 2m). \end{aligned}$$

We then make a shift in the last equation, multiply it by $q_1(x)$, and substitute the right-hand sides of the above equations

$$\begin{aligned} q_1(x)p(x+2) &= \sum_{l=1}^{2m} q_l(x+1)q_1(x)p_l(x+1) \\ &= \sum_{l=1}^{2m} q_l(x+1)q_{l1}(x)p(x+1) + \sum_{l=1}^{2m}\sum_{j=2}^{2m} q_l(x+1)q_{lj}^{(1)}(x)p_j(x) \\ &= \sum_{j=1}^{2m} q_j(x+1)q_{j1}(x)p(x+1) + \sum_{j=2}^{2m} q_j^{(1)}(x)p_j(x). \end{aligned}$$

We may now drop the equation for p_1 and continue with the rest.

(2) For p_2 to be the second pivot element,

$$q_{2n}^{(1)}(\mathbf{u}) = \sum_{l=1}^{2m} q_{l,n+1}(\mathbf{u})(q_{l2n}(\mathbf{u})q_{1n}(\mathbf{u}) - q_{l1n}(\mathbf{u})q_{2n}(\mathbf{u}))$$

must not be identically zero. Eliminating p_2 we get the equations

$$\begin{aligned} q_2^{(1)}(x)q_1(x)p_i(x+1) = &\sum_{j=3}^{2m} q_{ij}^{(2)}(x)p_j(x) \\ &+\text{terms involving } p(x+1) \text{ and } p(x+2) \end{aligned}$$

for $i = 2, \ldots, 2m$, and

$$\begin{aligned} q_2^{(1)}(x)q_1(x+1)p(x+3) = &\sum_{j=3}^{2m} q_j^{(2)}(x)p_j(x) \\ &+\text{terms involving } p(x+1) \text{ and } p(x+2). \end{aligned}$$

We may now drop the equation for p_2.

(3) Elimination is then continued as above, step by step.

(4) After the second to the last step we obtain

$$\begin{aligned} &q_{t-1}^{(t-2)}(x)\cdots q_2^{(1)}(x)q_1(x)p_i(x+1) \\ &\quad = \sum_{j=t}^{2m} q_{ij}^{(t-1)}(x)p_j(x) + \text{terms involving } p(x+1), \ldots, p(x+t-1) \end{aligned}$$

for $i = t-1, \ldots, 2m$, and

$$q_{t-1}^{(t-2)}(x) \cdots q_2^{(1)}(x+t-3) q_1(x+t-2)\, p(x+t) = \sum_{j=t}^{2m} q_j^{(t-1)}(x) p_j(x) + \text{terms involving } p(x+1), \ldots, p(x+t-1).$$

For p_t to be the last pivot element $q_{tn}^{(t-1)}(\mathbf{u})$ must not be identically zero.

(5) Finally, after the last step we obtain

$$q_t^{(t-1)}(x) \cdots q_2^{(1)}(x+t-2) q_1(x+t-1)\, p(x+t+1) = \sum_{j=t+1}^{2m} q_j^{(t)}(x) p_j(x) + \text{terms involving } p(x+1), \ldots, p(x+t).$$

Since the elimination procedure now cannot be continued, it is the case that $q_{jn}^{(t)}(\mathbf{u})$ ($j = t+1, \ldots, 2m$) are all identically zero, whence, by Lemma 9, $q_j^{(t)}(\mathbf{u}_0; x)$ ($j = t+1, \ldots, 2m$) all are identically zero, too, and we obtain the desired difference equation for $p(\mathbf{u}_0; x)$.

To indicate the choice of $\mathbf{u}_0$ we define the polynomial

$$Q_n(\mathbf{u}) = \prod_{j=1}^{t} q_{jn}^{(j-1)}(\mathbf{u}),$$

where we denote $q_{1n}^{(0)}(\mathbf{u}) = q_{1n}(\mathbf{u})$. For the elimination procedure to succeed, the sequence $(Q_n(\mathbf{u}))_{n=0}^{\infty}$ should not be identically zero. Any choice of $\mathbf{u}_0$ such that $Q_n(\mathbf{u}_0) \neq 0$ for some n will then be acceptable. It is observed that $Q_n(\mathbf{u})$ is of the form dealt with in the previous section, and thus it has a zero indicator $(G_n)_{n=0}^{\infty}$, and we may apply Lemma 10 to it.

We note next that each step in the elimination procedure is reversible, i.e., given the difference equation for $p(\mathbf{u}_0; x)$ and initial values for

$$p(\mathbf{u}_0; x), \quad x \in \bigcup_{n=N_0+1}^{N_0+t} (n, n+\varepsilon_N)$$

and

$$p_{t+1}(\mathbf{u}_0; x), \ldots, p_{2m}(\mathbf{u}_0; x), \quad N_0 < x < N_0 + \varepsilon_N$$

the reverse procedure recursively determines initial values for

$$p_1(\mathbf{u}_0; x), \ldots, p_t(\mathbf{u}_0; x), \quad N_0 < x < N_0 + \varepsilon_N,$$

such that the original difference system is satisfied for $x \in \bigcup_{n=N_0}^{N} (n, n+\varepsilon_N)$. A natural choice for the given initial values, remembering the goal we have in mind, is of course

$$p(\mathbf{u}_0; x) = 0 \quad \text{for } x \in \bigcup_{n=N_0+1}^{N_0+t} (n, n+\varepsilon_N)$$

and

$$p_j(\mathbf{u}_0; x) = p_{jN_0}(\mathbf{u}_0) \quad \text{for } N_0 < x < N_0 + \varepsilon_N \text{ and } j = t+1, \ldots, 2m.$$

We will use these initial values in the sequel. As a consequence,

$$p(\mathbf{u}_0; x) = 0 \quad \text{for } x \in \bigcup_{n=N_0+1}^{N} (n, n+\varepsilon_N).$$

A corresponding elimination (and reverse elimination) procedure may be carried out for the recurrence system

$$p_{i,n+1}(\mathbf{y}, \mathbf{u}) = \sum_{j=1}^{2m} q_{ijn}(\mathbf{u}) p_{jn}(\mathbf{y}, \mathbf{u}) \quad (i = 1, \ldots, 2m),$$
$$p_{n+1}(\mathbf{y}, \mathbf{u}) = \sum_{j=1}^{2m} q_{jn}(\mathbf{u}) p_{jn}(\mathbf{y}, \mathbf{u})$$

for values of n satisfying certain assumptions (we use a notation similar to the one above):
(1) In the first step $q_{1n}(\mathbf{u})$ should not be the zero polynomial.
(2) In the second step

$$q_{2n}^{(1)}(\mathbf{u}) = \sum_{l=1}^{2m} q_{l,n+1}(\mathbf{u})(q_{l2n}(\mathbf{u})q_{1n}(\mathbf{u}) - q_{l1n}(\mathbf{u})q_{2n}(\mathbf{u}))$$

should not be the zero polynomial.
(3) Etc. In the final step $q_{tn}^{(t-1)}(\mathbf{u})$ should not be the zero polynomial.
All in all, we see that the polynomial $Q_n(\mathbf{u})$, defined above, should not be the zero polynomial. We note that, for a fixed positive value $\mathbf{u}_0$ of $\mathbf{u}$, the process can be carried out, too, if $Q_n(\mathbf{u}_0) \neq 0$.

7. Existence of test set

To show existence of a test set we now proceed as follows (and it may be noted that Hilbert's Basissatz is not used here):
(1) Using the zero indicator $(G_n)_{n=0}^{\infty}$ of the sequence $(Q_n(\mathbf{u}))_{n=0}^{\infty}$, assumed not to be identically zero, we obtain an integer interval where a value $N_0 \geqslant 2m$ will be found such that $G_{N_0} \neq 0$. We then consider an arbitrary $N \geqslant N_0 + 2m$.
(2) We assume that $f\delta^n(w) = g\delta^n(w)$ for $n = 0, \ldots, N_0 + 2m$. This implies that $p_n(\mathbf{u})$ is the zero polynomial for $n = 0, \ldots, N_0 + 2m$, and that $[f\delta^n(w)] = [g\delta^n(w)]$ for $n \geqslant 0$.
(3) Assuming that $Q_{N_0}(\mathbf{u}_0) \neq 0$ we go through the elimination procedure. Using the initial values

$$p(\mathbf{u}_0; x) = 0 \quad \text{for } x \in \bigcup_{n=N_0+1}^{N_0+t} [n, n+\varepsilon_N)$$

and

$$p_j(\mathbf{u}_0; x) = p_{jN_0}(\mathbf{u}_0) \quad \text{for } N_0 \leqslant x < N_0 + \varepsilon_N \text{ and } j = t+1, \ldots, 2m,$$

reverse elimination for the difference system then gives us the functions

$$p_1(\mathbf{u}_0; x), \ldots, p_{2m}(\mathbf{u}_0; x),$$

which are *continuous on the half-open interval* $[N_0, N_0+\varepsilon_N)$ and thus satisfy $p_j(\mathbf{u}_0; N_0) = p_{jN_0}(\mathbf{u}_0)$.

(4) Using these as initial values for the difference system we get the *continuous* functions $p_1(\mathbf{u}_0; x), \ldots, p_{2m}(\mathbf{u}_0; x)$ and $p(\mathbf{u}_0; x)$ on the set

$$\bigcup_{n=N_0+1}^{\infty} [n, n+\varepsilon_N)$$

satisfying $p_j(\mathbf{u}_0; n) = p_{jn}(\mathbf{u}_0)$ and $p(\mathbf{u}_0; n) = p_n(\mathbf{u}_0)$ for $n \geqslant N_0 + 1$.

(5) Applying the difference equation for $p(\mathbf{u}_0; x)$ obtained via the elimination procedure, we see that

$$p(\mathbf{u}_0; x) = 0 \quad \text{for } x \in \bigcup_{n=N_0+1}^{N} (n, n+\varepsilon_N).$$

(6) By continuity, it follows that:

$$p(\mathbf{u}_0; x) = 0 \quad \text{for } x \in \bigcup_{n=N_0+1}^{N} [n, n+\varepsilon_N)$$

and hence that $p_n(\mathbf{u}_0) = 0$ for $n = 0, \ldots, N$.

(7) Since N was arbitrary, it follows that $p_n(\mathbf{u}_0) = 0$ for $n \geqslant 0$.

(8) Letting $\mathbf{u}_0$ go through all positive points of the Zariski open set

$$\{\mathbf{u} \mid Q_{N_0}(\mathbf{u}) \neq 0\}$$

we finally conclude that $p_n(\mathbf{u})$ is the zero polynomial for all n, which means that $f\delta^n(w) = g\delta^n(w)$ for $n \geqslant 0$.

(9) Since N_0 does not depend on f and g, and $t \leqslant 2m$, the set

$$T = \{\delta^n(w) \mid n = 0, \ldots, N_0 + 2m\}$$

thus is a finite test set for $\{\delta^n(w) \mid n \geqslant 0\}$. (Where we assume that a proper decomposition is already made.)

It remains to find an upper bound for N_0.

8. Estimating the upper bound

To get an upper bound for the N_0 in the previous section, we first denote by $|v|$ the *length* of an element of G_Σ, that is, the minimum number of occurrences of generators and their

inverses needed to express v. Further we denote

$$|\delta| = \max_{i=1}^{m} |\delta(a_i)| \quad \text{and} \quad M = \max(|\delta|, 2|w|).$$

We have then (see Section 5)

$$\text{max-trace}(q_{ijn}(\mathbf{u})) \leqslant M \quad (i = 1, \ldots, 2m;\ j = 1, \ldots, 2m)$$

and

$$\text{max-trace}(q_{jn}(\mathbf{u})) \leqslant M \quad (j = 1, \ldots, 2m).$$

(Recall that these max-traces do not depend on n, nor on f or g.)

We then get recursively an upper bound M_l for max-trace $\left(q_{jn}^{(l)}(\mathbf{u})\right)$ as follows. During an elimination step the following polynomial operations are carried out (the resulting upper bound for the max-trace is given in parenthesis, see Lemma 7):

- the first equations are multiplied by a coefficient appearing on the right-hand side of the last equation ($2M_l^2$),
- the last equation is solved for a term corresponding to the coefficient which is then substituted in the first equations ($2 \times 2M_l^2$),
- the last equation is shifted and then multiplied by the same coefficient, and
- right-hand sides of the first equations are substituted in the last equation and the resulting expression is multiplied out ($2m \times 2 \times M_l \times 4M_l^2$).

We have thus the recursion

$$\begin{aligned} M_0 &= M, \\ M_{l+1} &= 16m M_l^3 \end{aligned}$$

the solution of which is

$$M_l = (16m)^{\frac{3^l-1}{2}} M^{3^l}.$$

Noting that $t \leqslant 2m$, we thus get for the max-trace of $Q_n(\mathbf{u})$ the upper bound

$$R = 2^{2m-1} \prod_{l=0}^{2m-1} M_l = 2^{2m-1} (16m)^{\frac{3^{2m}-4m-1}{4}} M^{\frac{3^{2m}-1}{2}}.$$

From Section 5 we then obtain a corresponding upper bound T for the order of an LHRCC satisfied by $(G_n)_{n=0}^{\infty}$, the zero indicator of $Q_n(\mathbf{u})$, and this is also the upper bound for the number N_0. We have

$$T = \binom{R! + D - 1}{D - 1} (2(s-1)R! + 1),$$

where s is the maximum multiplicity of characteristic roots of $\mathcal{L}$, $D = \frac{1}{2}d(d+1)$ and d is the number of distinct characteristic roots of $\mathcal{L}$. Including the factor $K!$ needed for the decomposition we get the upper bound

$$K!(T + 2m) + m.$$

We have now proved our main result (note that Magnus representation is valid for free monoids as well):

Theorem 11. *In the free metabelian group* (*resp. free monoid*) *generated by the m elements* $a_1, \ldots, a_m$, *the set*

$$\{\delta^n(w) \mid n = 0, \ldots, N\}$$

is a finite test set for the iterated morphism $\{\delta^n(w) \mid n \geqslant 0\}$ *if*

$$N \geqslant K!(T + 2m) + m,$$

where

$$K = \left\lfloor e^{2m\sqrt{3\ln m}} \right\rfloor, \quad T = \binom{R! + D - 1}{D - 1} (2(s-1)R! + 1),$$
$$R = 2^{2m-1}(16m)^{\frac{3^{2m}-4m-1}{4}} M^{\frac{3^{2m}-1}{2}}, \quad D = \frac{1}{2}d(d+1),$$
$$M = \max(|\delta(a_1)|, \ldots, |\delta(a_m)|, 2|w|),$$

d is the number of distinct nonzero eigenvalues of $[\delta]^{K!}$, *and s is the maximum multiplicity of these eigenvalues.*

A "more explicit" upper bound is obtained by setting $s = d = m$. We note also that for $d = 1$ we have $D = 1$, $s = m$ and

$$T = 2(m-1)R! + 1$$

and that for $s = 1$ we have $d = m$, $D = \frac{1}{2}m(m+1)$ and

$$T = \binom{R! + D - 1}{D - 1}.$$

9. Applications and variants

For the case of free monoids there is an immediate implication concerning the HD0L sequence equivalence problem. Take two HD0L sequences

$$(f\delta_1^n(w_1))_{n=0}^{\infty} \quad \text{and} \quad (g\delta_2^n(w_2))_{n=0}^{\infty},$$

where $\delta_1 : \Sigma_1^* \longrightarrow \Sigma_1^*$ and $\delta_2 : \Sigma_2^* \longrightarrow \Sigma_2^*$ are endomorphisms, $f : \Sigma_1^* \longrightarrow \Delta^*$ and $g : \Sigma_2^* \longrightarrow \Delta^*$ are morphisms, $w_1 \in \Sigma_1^*$ and $w_2 \in \Sigma_2^*$. We denote the cardinalities of Σ_1 and Σ_2 by m_1 and m_2, respectively, and

$$k = m_1 + m_2 \quad \text{and} \quad M = \max(|\delta_1|, |\delta_2|, |w_1| + |w_2|).$$

Further we denote by d the joint number of distinct nonzero eigenvalues of $[\delta_1]^{K!}$ and $[\delta_2]^{K!}$ where

$$K = \left\lfloor e^{2k\sqrt{3\ln k}} \right\rfloor$$

and by s the maximum multiplicity of these eigenvalues.

By slightly changing the constructs in the previous sections we see that the result corresponding to Theorem 11 is now the following:

$$f\delta_1^n(w_1) = g\delta_2^n(w_2) \quad (n \geqslant 0)$$

if and only if

$$f\delta_1^n(w_1) = g\delta_2^n(w_2) \quad (n = 0, \ldots, K!(T+k)+k),$$

where

$$T = \binom{R! + D - 1}{D - 1}(2(s-1)R! + 1),$$
$$R = 2^{k-1}(8k)^{\frac{3^k-2k-1}{4}} M^{\frac{3^k-1}{2}} \quad \text{and} \quad D = \frac{1}{2}d(d+1).$$

(A "more explicit" upper bound is obtained by setting $s = d = k$.) It may be noted that a lower bound for the number of terms to be checked is known to be $\Omega(k^4)$, see [21].

The above bound obviously does not depend on f or g. It is thus in particular valid for checking equivalence of the D0L sequences

$$(\delta_1^n(w_1))_{n=0}^{\infty} \quad \text{and} \quad (\delta_2^n(w_2))_{n=0}^{\infty}$$

and is then much smaller than the previously known best bound, obtained by Ehrenfeucht and Rozenberg [7]. For the D0L sequence equivalence the still much smaller bound k (in our notation) is conjectured—this is often referred to as the "$2n$-conjecture". So far the conjecture has been proved only for the binary case where $m_1 = m_2 = 2$, see [16]. On the other hand, relatively small upper bounds have been obtained also for D0L sequences of other special types, see e.g. [12,13].

It is not difficult to see that the constructs in the previous sections can be carried out for any metabelian group (or any monoid) generated by finitely many matrices of the form

$$\begin{pmatrix} 1 & 0 \\ p(\mathbf{y}, \mathbf{u}) & \mathbf{u}^{\mathbf{a}} \end{pmatrix},$$

where $\mathbf{a}$ is an integer valued multi-index and $p(\mathbf{y}, \mathbf{u})$ is a Laurent polynomial with integer coefficients. For example, the generator sets

$$\begin{pmatrix} 1 & 0 \\ y_j & u \end{pmatrix} (j = 1, \ldots, r) \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & u_j \end{pmatrix} (j = 1, \ldots, r)$$

both generate metabelian groups which are not free. The monoids they generate are however free and thus these generator sets would suffice to deal with HD0L sequences. As another

example take the sets

$$\begin{pmatrix} 1 & 0 \\ y_j & 1 \end{pmatrix} \ (j = 1, \ldots, r) \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & u_j \end{pmatrix} \ (j = 1, \ldots, r),$$

where both generate the free Abelian group (or monoid). For these sets, the constructs in the previous sections can be simplified a lot, and the well-known bound $2m$ is obtained. Using mixtures of the above two generator types one obtains "partially commutative monoids", etc.

References

[1] M.H. Albert, J. Lawrence, A proof of Ehrenfeucht's conjecture, Theoret. Comput. Sci. 41 (1985) 121–123.
[2] G. Baumschlag, F.B. Cannonito, D.J.S. Robinson, The algorithmic theory of finitely generated metabelian groups, Trans. Amer. Math. Soc. 344 (1994) 629–648.
[3] J. Berstel, M. Mignotte, Deux problèmes décidables des suites récurrentes linéaires, Bull. Soc. Math. France 104 (1976) 175–184.
[4] J. Berstel, C. Reutenauer, Rational Series and Their Languages, Springer, Verlag, 1988.
[5] V.D. Blondel, N. Portier, The presence of a zero in an integer linear recurrent sequence is NP-hard to decide, Linear Algebra Appl. 351–352 (2002) 91–98.
[6] M. Buck, N. Zierler, Decimations of linearly recurring sequences, Comput. Math. Appl. 39 (2000) 95–102.
[7] A. Ehrenfeucht, G. Rozenberg, On a bound for the D0L sequence equivalence problem, Theoret. Comput. Sci. 12 (1980) 339–342.
[8] V. Guba, The equivalence of infinite systems of equations in free groups and semigroups to finite subsystems, Mat. Zametki 40 (1986) 321–324 (in Russian).
[9] P. Hall, Finiteness conditions for soluble groups, Proc. London Math. Soc. (3) 4 (1954) 419–436.
[10] G. Hansel, Une dèmonstration simple du thèoréme de Skolem–Mahler–Lech, Theoret. Comput. Sci. 244 (1986) 91–98.
[11] Š. Holub, Binary equality sets are generated by two words, J. Algebra 259 (2003) 1–42.
[12] J. Honkala, A polynomial bound for certain cases of the D0L sequence equivalence problem, Theory Comput. Syst. 34 (2001) 263–272.
[13] J. Honkala, On the equivalence problem of polynomially bounded D0L systems—a bound depending only on the size of the alphabet, Theory Comput. Syst. 36 (2003) 89–103.
[14] J. Honkala, K. Ruohonen, On the images of $\mathbb{N}$-rational sequences counting multiplicities, Internat. J. Algebra Comput. 12 (2003) 303–321.
[15] N. Jacobson, Basic Algebra, W.H. Freeman, New York, 1989.
[16] J. Karhumäki, On the equivalence problem for binary D0L systems, Inform. and Control 50 (1981) 276–284.
[17] D.J. Lewis, Diophantine equations: p-adic methods, in: W.J. LeVeque (Ed.), Studies in Number Theory, MAA, 1969, pp. 25–75.
[18] M. Lothaire, Algebraic Combinatorics on Words, Cambridge University Press, Cambridge, 2002.
[19] W. Magnus, On a theorem of Marshall Hall, Ann. Math. 40 (1954) 764–768.
[20] G.S. Makanin, Decidability of the universal and positive theories of a free group, Izv. Ross. Akad. Nauk Ser. Mat. 48 (1985) 735–749 (in Russian).
[21] W. Plandowski, The complexity of the morphism equivalence problem for context-free languages, Ph.D. Thesis, Warsaw University, 1995.
[22] W. Plandowski, Test sets for large families of languages, in: Z. Ésik, Z. Fülöp (Eds.), Developments in Language Theory '03, Lecture Notes in Computer Science, Vol. 2710, Springer, Berlin, 2003, pp. 75–94.
[23] P. Prusinkiewicz, A. Lindenmayer, The Algorithmic Beauty of Plants, Springer, Berlin, 1990.
[24] D.J.S. Robinson, A Course in the Theory of Groups, Springer, Berlin, 1980.
[25] G. Rozenberg, A. Salomaa, The Mathematical Theory of L Systems, Academic Press, New York, 1980.
[26] G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, Vol. 1, Word, Language, Grammar, Springer, Berlin, 1997.

[27] G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, Vol. 3, Beyond Words, Springer, Berlin, 1997.
[28] K. Ruohonen, Test sets for iterated morphisms, Mathematics Report 49, Tampere University of Technology, 1986.
[29] K. Ruohonen, Solving equivalence of recurrent sequences in groups by polynomial manipulation, Fund. Inform. 38 (1999) 135–148.
[30] A. Salomaa, M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer, Berlin, 1978.
[31] W.M. Schmidt, The zero multiplicity of linear recurrence sequences, Acta Math. 182 (1999) 243–282.
[32] N.K. Vereshchagin, On the zeros of linear recurrent sequences, Dokl. Akad. Nauk 278 (1984) 502–505 (in Russian).